Cisco Secure Boot and Trust Anchor Module Differentiation

Cisco® Trust Anchor Technologies provide the foundation for Cisco Trustworthy Systems. Cisco Secure Boot helps ensure that the code running on Cisco hardware platforms is authentic and unmodified. The Cisco Trust Anchor module helps verify that Cisco hardware is authentic and provides additional security services.

Cisco Trustworthy Systems differentiate Cisco in the marketplace in the area of platform integrity, including:

- Cisco hardware-anchored Secure Boot and the Unified Extensible Firmware Interface (UEFI) Secure Boot
- Cisco Trust Anchor module (TAm) and the Trusted Platform Module (TPM)

Cisco Secure Boot and UEFI Secure Boot

When it comes to software authentication, Cisco is differentiated by anchoring the Secure Boot process in hardware, thus providing the most robust security (Figure 1). It is robust because hardware modification is difficult, expensive, and not easy to conceal, even if the hacker has physical possession of the device.

Figure 1. Anchoring the Secure Boot in Hardware
With a hardware-anchored Secure Boot, the first instructions that run on a CPU are stored in immutable hardware. They cannot be tampered with, or they are validated by the hardware. When the device boots, the microloader verifies that the next set of instructions is genuine Cisco by validating the Cisco digital signature on that set of instructions.

Next, the genuine bootloader validates that the operating system (OS) is also genuine Cisco by checking that it was digitally signed by Cisco.

This process creates a “chain of trust” from microloader through bootloader to the operating system, establishing the authenticity of the software.

These digital signature checks are cryptographically secure. It is not mathematically feasible to alter the software without that modification being detected when the signatures are validated.

If any digital signature check fails, the Cisco device will not let that software boot, so that malicious code will not run.

**Cisco Secure Boot**

- Anchors Secure Boot process to hardware
- Resists tampering attacks in the supply chain and on firmware in physical possession
  - More difficult to modify hardware than software
  - More expensive
  - More visible

Conversely, with the industry-standard UEFI Secure Boot, there is no anchor in hardware. The chain of trust does not begin until the bootloader stage (Figure 2).
Figure 2. Comparison of Cisco and UEFI Secure Boot Chains of Trust

UEFI Secure Boot may be suitable for less mission-critical scenarios, but you will face a greater risk of malicious rootkits being inserted. Bootloader rootkits are instructions that can be stored in hardware that is not immutable. They are activated for malicious purposes when the device is next booted. These instructions can be inserted at any time, even during the supply chain transfer.

**Unified Extensible Firmware Interface (UEFI)**

- Not anchored in hardware
- Nothing validates BIOS
  - Susceptible to BIOS rootkits
  - Susceptible to easy modifications in supply chain or with physical possession

**Cisco Trust Anchor Module and Trusted Platform Module**

The Cisco Trust Anchor module and the Trusted Platform Module are based on the Trusted Computing Group industry standard. They have similar capabilities. These include anti-tamper protection; highly secure storage; policy and configuration; and cryptographic services (Figure 3).
When the Cisco hardware-anchored Secure Boot has authenticated the software as genuine Cisco in a Cisco device with the TAm, the operating system then queries the TAm to verify that the hardware is authentic. It does this by cryptographically checking the TAm for a secure unique device identifier (SUDI) that could have come only from Cisco.

The SUDI is permanently programmed into the TAm and logged by Cisco during Cisco’s closed, secured, and audited manufacturing processes. This programming provides strong supply chain security, which is particularly important for embedded systems like routers and switches.

**Cisco Trust Anchor Module (TAm)**
- Hardware designed to provide both end-user and supply chain protections
  - End-user protections include highly secure storage of user credentials, passwords, settings
  - Supply chain protections – Cisco SUDI (secure unique device identifier) inserted during manufacturing
- Secured at manufacturing → no user intervention required
- Ideal for embedded computing like routers and Wi-Fi access points

In contrast, although the industry-standard TPM has similar functions to those of the TAm, it is not typically permanently programmed during manufacture with a unique device identifier, which is left to the end user. This process requires user intervention and development, but it provides flexibility, which is especially useful for general or multiple-purpose computing devices like servers and computers. However, the risk for supply chain modifications is also greater.

**Trusted Platform Module (TPM)**
- Typically focused on providing end-user capabilities
  - Hardware protection for user certificates
  - Hardware protection for integrity information
- Custom development required for use
- Ideal for general-purpose computing like servers and PCs
Industry Standards and Cisco Enhancements

Cisco is a strong supporter of the Trusted Computing Group and Unified Extensible Firmware Interface standards for platform security. We participate in the defining of such standards, often based on our pioneering and industry-leading developments in each area. Trustworthy technologies like hardware-based Secure Boot and the Trust Anchor module establish Cisco as an industry leader in the area of platform integrity, providing our customers with a foundation of trust that their Cisco devices are authentic and operating as intended. As threats evolve, we are committed to ongoing innovation and leadership to address the ever-growing cybersecurity threat landscape.

For More Information

Read more about security and trust at trust.cisco.com.

Send inquiries to ask-trustworthy@cisco.com.